Bridge Certification Authority Technology Demonstration Phase 2 — Results and Lessons Learned

Presentation to the FPKI TWG

David Lemire

A&N Associates, Inc.

2 August 2001

Results (1)

- Demonstrated Technical Feasibility
  - Achieve Cross-Certification with Five Distinct CA Products
  - Successful Mixing of Hierarchical and Mesh PKIs
  - Used COTS PKIs for Both Web and Messaging
  - Excellent Interoperability Among Messaging Clients
  - Proper Processing of Advanced Certification Path Features (e.g., Policies, Name Constraints)

Results (2)

- Directory Lookup Key Performance Factor
  - Certificate Caching Dramatically Improves Performance
- Succeeded in Demonstrating Advanced Access Control Based on Attribute Certificates
  - Worked in Both Web and Messaging Environments
  - Permitted Rapid Update of Subscriber Authorizations

Lessons Learned (1)

- Internet Adage of "Strict in What You Send, Liberal in What You Process" is Applicable to Certificates, CRLs, and S/MIME
- Directory Chaining Requires Careful / Detailed Configuration & Troubleshooting
  - Clock Synchronization is One Key
- Still Differing Interpretations of Forward/Reverse in Cross-Certificates

Lessons Learned (2)

- Conflicting Views of Processing Extensions in Trust Anchor Certificates
- Inconsistent / Incompatible Computing of Key Identifiers Caused Path Discovery to Fail
- Multi-vendor Community Worked Together Well
  - Communication, Coordination, Community Helps The Demo
  - Mail Lists and Bi-Monthly Status Meetings Kept Communication Flowing

Mail Client S/MIME v3 Signed-And-Encrypted Interoperability

Signed and Encrypted Results

		Receiving Client		
		Baltimore	Entrust	CygnaCom
Sending Client	Baltimore		Works	Works
	Entrust	Works		Works
	CygnaCom	Works	Fails	

- The Entrust client is unable to process a multipart signed message encapsulated in the envelopedData of a signed and encrypted message
- The CygnaCom client always generates signed messages in a multipart format
- The Baltimore client generates signed messages as a single part, but is able to process both single as well as multipart signed messages

A&V Associates, Inc.

Back to Dave Fillingham . . .